



Негосударственное частное учреждение
Профессиональная образовательная организация
«Уральский институт подготовки кадров «21-й век»

УТВЕРЖДАЮ:

Председатель учебно-методического
совета первый проректор по учебной
работе и инновациям

_____ М.В. Федорук

«_____» _____ 20____ г.

ПРОГРАММА
ИТОГОВОЙ аттестации
по специальности

10.02.01 «Организация и технология защиты информации»

Нижний Тагил, 2015 г.

Программа итоговой аттестации разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.01 «Организация и технология защиты информации»

Организация-разработчик НЧУ ПОО «Уральский институт подготовки кадров «21-й век»

Составитель: к.п.н., доцент Райхерт Т.Н.

Программа рассмотрена и утверждена на заседании кафедры
« ___ » _____ 2015 г. протокол № ___

Зав. кафедрой _____

Введение

Настоящая программа итоговой аттестации (ИА) разработана в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.01 «Организация и технология защиты информации» (приказ № 805 Министерства образования и науки Российской Федерации от 28 июля 2014 года), Федерального закона от 29.12.2012 № 273-ФЗ (ред. от 13.07.2015) «Об образовании в Российской Федерации» (с изм. и доп., вступ. в силу с 24.07.2015) и Приказа Министерства образования и науки Российской Федерации (Минобрнауки России) от 16 августа 2013 г. № 968 г. Москва «Об утверждении Порядка проведения итоговой аттестации по образовательным программам среднего профессионального образования», Уставом Негосударственного частного учреждения профессионально образовательной организации «Уральский институт подготовки кадров «21-й век» (далее - Институт), Положением об итоговой аттестации выпускников Института.

1. Цель и задачи выпускной квалификационной работы

1.1. Выпускные квалификационные работы выполняются в формах, соответствующих определенным ступеням (уровням) среднего образования - в форме дипломной работы.

Дипломные работы могут основываться на обобщении выполненных курсовых работ и подготовиться к защите в завершающий период теоретического обучения.

1.2. Выполнение выпускных квалификационных работ является заключительным этапом обучения студентов в Институте и имеет своей целью систематизацию, обобщение и закрепление теоретических знаний, практических умений и навыков.

1.3. Выпускные квалификационные работы выполняются на последнем курсе обучения в сроки, определенные учебным планом и графиком учебного процесса.

1.4. Необходимым условием допуска к итоговой аттестации является представление документов, подтверждающих освоение обучающимся компетенций при изучении теоретического материала и прохождении практики по каждому из основных видов профессиональной деятельности.

1.6. Программа ИА и приказ о закреплении тем дипломных работ доводятся до сведения студентов не позднее шести месяцев до начала ИА. К итоговой аттестации допускаются лица, не имеющие академической задолженности и в полном объеме выполнившие учебный план или индивидуальный учебный план, предусмотренные программой подготовки специалистов среднего звена по специальности «Организация и технология защиты информации». ИА выпускника Института по специальности «Организация и технология защиты информации» включает подготовку и защиту дипломной работы. Подготовка к ИА - с 38 по 41 неделю (4 недели),

проведение ИА - с 42 по 43 неделю (2 недели) четвертого курса обучения.

1.7. ИА проводится экзаменационной комиссией (ГЭК). Целью работы ГЭК является определение соответствия студентами программы подготовки специалистов среднего звена (ППССЗ) соответствующим требованиям Федерального государственного образовательного стандарта среднего профессионального образования по специальности 01.02.01 «Организация и технология защиты информации» базового уровня подготовки.

1.8. Лицам, не проходившим итоговую аттестацию по уважительной причине, предоставляется возможность пройти итоговую аттестацию без отчисления из Института.

Дополнительные заседания экзаменационных комиссий организуются в установленные Институтом сроки, но не позднее четырех месяцев после подачи заявления лицом, не проходившим итоговой аттестации по уважительной причине.

1.9. Обучающиеся, не прошедшие итоговую аттестацию или получившие на итоговой аттестации неудовлетворительные результаты, проходят итоговую аттестацию не ранее чем через шесть месяцев после прохождения итоговой аттестации впервые.

1.10. Для прохождения итоговой аттестации лицо, не прошедшее итоговую аттестацию по неуважительной причине или получившее на итоговой аттестации неудовлетворительную оценку, восстанавливается в Институт на период времени, установленный Институтом самостоятельно, но не менее предусмотренного календарным учебным графиком для прохождения итоговой аттестации, соответствующей ППССЗ.

Повторное прохождение итоговой аттестации для одного лица назначается Институтом не более двух раз.

2. Требования к результатам освоения образовательной программы (перечень компетенций с указанием знаний, умений и навыков практического опыта)

В процессе защиты ВКР выпускник должен продемонстрировать владение:

2.1 общими компетенциями, включающими в себя способность:

- понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности (ОК 1);
- организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество (ОК 2);
- принимать решения в стандартных и нестандартных ситуациях и

нести за них ответственность (ОК 3);

- осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития (ОК 4)

- использовать информационно-коммуникационные технологии в профессиональной деятельности (ОК 5);

- работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями (ОК 6);

- брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий (ОК 7);

- самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации (ОК 8);

- ориентироваться в условиях частой смены технологий в профессиональной деятельности (ОК 9);

- применять математический аппарат для решения профессиональных задач (ОК 10);

- оценивать значимость документов, применяемых в профессиональной деятельности (ОК 11);

- ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность (ОК 12).

2.2. профессиональными компетенциями, соответствующими видами деятельности:

2.2.1. Участие в планировании и организации работ по обеспечению защиты объекта:

- участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации (ПК1.1);

- участвовать в разработке программ и методик организации защиты информации на объекте (ПК 1.2);

- осуществлять планирование и организацию выполнения мероприятий по защите информации (ПК 1.3);

- участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности (ПК 1.4);

- вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации (ПК 1.5);

- обеспечивать технику безопасности при проведении организационно-технических мероприятий (ПК 1.6);

- участвовать в организации и проведении проверок объектов информатизации, подлежащих защите (ПК 1.7);
- проводить контроль соблюдения персоналом требований режима защиты информации (ПК 1.8);
- участвовать в оценке качества защиты объекта (ПК 1.9).

2.2.2. Организация и технология работы с конфиденциальными документами:

- участвовать в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации (ПК 2.1);
- участвовать в организации и обеспечивать технологию ведения делопроизводства с учетом конфиденциальности информации (ПК 2.2);
- организовывать документооборот, в том числе электронный, с учетом конфиденциальности информации (ПК 2.3);
- организовывать архивное хранение конфиденциальных документов (ПК 2.4);
- оформлять документацию по оперативному управлению средствами защиты информации и персоналом (ПК 2.5);
- вести учет работ и объектов, подлежащих защите (ПК 2.6);
- подготавливать отчетную документацию, связанную с эксплуатацией средств контроля и защиты информации (ПК 2.7);
- документировать ход и результаты служебного расследования (ПК 2.8);
- использовать нормативные правовые акты, нормативно-методические документы по защите информации (ПК 2.9).

2.2.3. Применение программно-аппаратных и технических средств защиты информации:

- применять программно-аппаратные и технические средства защиты информации на защищаемых объектах (ПК 3.1);
- участвовать в эксплуатации систем и средств защиты информации защищаемых объектов (ПК 3.2);
- проводить регламентные работы и фиксировать отказы средств защиты (ПК 3.3);
- выявлять и анализировать возможные угрозы информационной безопасности объектов (ПК 3.4).

3. Состав итоговых испытаний включает выпускную квалификационную работу

3.1. В соответствии с требованиями Федерального Государственного образовательного стандарта дипломная работа техника по защите информации по специальности 10.02.01 «Организация и технология защиты информации» представляет собой законченную разработку в профессиональной области, в

которой:

- сформулирована актуальность и место решаемой задачи по защите информации в предметной области;
- проанализированы литература и информация по организации и используемых технологий по защите информации в данной области или в смежных предметных областях;
- определены и конкретно описаны выбранные дипломантом объемы, методы и средства решаемой задачи, иллюстрируемые данными и нормативными документами, используемые при реализации поставленной задачи по защите информации в предметной области;
- проанализированы предлагаемые пути, способы решения поставленных задач, а также оценивается экономическая, техническая и (или) социальная эффективность их внедрения в реальную информационную среду применения.

В соответствии с перечисленными требованиями в общем случае в дипломной работе студент-дипломник должен:

- обосновать актуальность и значимость решаемой задачи по обеспечению защиты выбранного информационного объекта;
- выполнить анализ литературы по вопросам выбранной темы работы;
- сформулировать сущность задачи по защите информации;
- провести аудит информационной безопасности защищаемого объекта;
- выявить возможные каналы утечки исследуемого объекта информатизации;
- разработать систему защиты информации (СЗИ) согласно нормативно-методических документов;
- обосновать выбор средств защиты информации;
- разработать мероприятия по внедрению СЗИ на объекте и предложить методику применения выбранных средств защиты;
- выполнить экономические расчеты (расчет экономической эффективности внедрения результатов работы, или расчет каких-либо других экономических показателей), характеризующих целесообразность внедрения предлагаемых мероприятий по защите информации.

3.2. Общими требованиями к дипломной работе являются:

- целевая направленность;
- четкость построения;
- логическая последовательность изложения материала;
- убедительность аргументаций;
- краткость и точность формулировок;
- конкретность изложения результатов работы;
- доказательность выводов и обоснованность рекомендаций;
- грамотное оформление.

3.3. Структурными элементами дипломной работы являются:

1. Титульный лист.
2. План и график выполнения дипломной работы.
3. Содержание.
4. Введение.
5. Основная часть (главы, параграфы, пункты).
6. Заключение.
7. Список использованных источников.
8. Приложения.
9. Презентация, демонстрационный материал

3.4. Дипломная работа может иметь исследовательский характер или представлять собой решение практической задачи одной из актуальных проблем специальности в области защиты информации и обеспечения информационной безопасности выбранного объекта.

3.5. Объектами дипломной работы могут быть методы и средства защиты информации, методы анализа уязвимости информации объектов, методы обоснования надежности (достаточности) выбранных мер защиты информации, методы экономической оценки эффективности предлагаемых защитных мероприятий и т.д.

3.6.

4. Описание показателей, критериев, шкалы оценивания компетенций

4.1. Дипломная работа призвана способствовать систематизации и закреплению знаний студента по специальности при решении конкретных задач. Защита дипломной работы проводится с целью выявления соответствия подготовки выпускника требованиям ФГОС по специальности и дополнительным требованиям Института (если они имеются), а также выявления уровня подготовки выпускника к самостоятельной профессиональной деятельности.

4.2. В критерии оценки уровня подготовки студента по специальности входит:

- соответствие тематики дипломной работы содержанию одного или нескольких профессиональных модулей, ее актуальность, оригинальность и новизна, полнота раскрытия темы;
- качество обзора литературы и источников и его соответствие выбранной теме дипломной работы;
- актуальность, оригинальность, новизна, практическая ценность задач экспериментальной части, их соответствие теме исследования, полнота и качество раскрытия поставленных задач;
- соответствие оформления дипломной работы установленным нормам и требованиям;
- уровень освоения общих и профессиональных компетенций, предусмотренных ФГОС, учебными программами дисциплин и профессиональных модулей, продемонстрированный студентом при защите дипломной работы и ответе на дополнительные вопросы;

- уровень практических умений и результатов приобретенного практического опыта, продемонстрированных выпускником при защите дипломной работы;

- готовность к конкретным видам профессиональной деятельности техника по защите информации, уровень знаний и умений, позволяющий решать ситуационные (профессиональные) задачи, давать ответы на вопросы экзаменационной комиссии; обоснованность, четкость, краткость ответов.

4.3. Защита выпускной квалификационной работы заканчивается выставлением оценок. При определении окончательной оценки по защите дипломной работы учитываются следующие показатели:

- соответствие представленной дипломной работы установленным критериям;

- доклад выпускника по каждому разделу работы;

- ответы на вопросы;

- оценка оппонента;

- отзыв научного руководителя.

- отчеты о ранее достигнутых результатах, дополнительные сертификаты, свидетельства (дипломы) олимпиад, конкурсов, творческие работы по специальности, характеристики с мест прохождения преддипломной практики.

Критерии оценки.

Результаты дипломной работы определяются оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» за ВКР выставляется, если дипломная работа носит исследовательский характер, имеет грамотно изложенную теоретическую главу, глубокий теоретический анализ, критический обзор практики, логичное, последовательное изложение материала с соответствующими выводами и обоснованными предложениями; имеет положительные отзывы научного руководителя и рецензента. При защите ВКР на «отлично» обучающийся - выпускник показывает глубокое знание вопросов темы, свободно оперирует данными исследования, вносит обоснованные предложения, а во время доклада использует наглядные пособия (презентацию PowerPoint, таблицы, схемы, графики и т. п.) или раздаточный материал, легко отвечает на поставленные вопросы.

Оценка «хорошо» за ВКР выставляется, если дипломная работа носит исследовательский характер, имеет грамотно изложенную теоретическую главу, в ней представлены достаточно подробный анализ и критический разбор практической деятельности, последовательное изложение материала с соответствующими выводами, но предложения студента недостаточно обоснованы. ВКР имеет положительный отзыв научного руководителя и рецензента. При ее защите обучающийся - выпускник показывает знание вопросов темы, оперирует данными исследования, вносит предложения по теме исследования, во время доклада использует наглядные пособия (презентацию PowerPoint, таблицы, схемы, графики и т. п.) или раздаточный материал, без особых затруднений отвечает на поставленные вопросы.

Оценка «удовлетворительно» за ВКР выставляется, если дипломная работа носит исследовательский характер, имеет теоретическую главу, базируется на практическом материале, но имеет поверхностный анализ и недостаточно критический разбор, в ней обнаружена непоследовательность изложения материала, представлены необоснованные предложения. В отзывах рецензентов имеются замечания по содержанию работы и методике анализа. При защите такой ВКР обучающийся - выпускник проявляет неуверенность, показывает слабое знание вопросов темы, не всегда дает исчерпывающие аргументированные ответы на заданные вопросы.

Оценка «неудовлетворительно» выставляется в случае полного несоответствия дипломной работы установленным требованиям, в процессе защиты студент не владеет теоретическим и практически материалом, наглядный материал не представлен. В отзывах научного руководителя и рецензента имеются критические замечания. При защите ВКР обучающийся - выпускник затрудняется отвечать на поставленные вопросы по ее теме, не знает теории вопроса, при ответе допускает существенные ошибки. К защите не подготовлены наглядные пособия и раздаточный материал.

Таким образом, при определении окончательной оценки за ВКР членами ГЭК учитываются:

- качество доклада выпускника;
- представленный им иллюстративный материал;
- мобильность выпускника и его грамотность при ответах на вопросы;
- оценка ВКР рецензентом;
- отзыв руководителя ВКР.

5. Порядок подготовки выпускной квалификационной работе

5.1. Типовые материалы, необходимые для оценки результатов освоения образовательной программы:

5.1.1. На заседания ГЭК представляются следующие документы:

- Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.01 «Организация и технология защиты информации»;
- программа ИА;
- приказ ректора Института о допуске студентов к ИА;
- приказ ректора Института об утверждении тематики дипломных работ по специальности, научных руководителей дипломных работ и оппонентов;
- задания к дипломным работам выпускников, подписанные научными руководителями и выпускниками, утвержденные заведующим кафедрой организации и технологии защиты информации;
- завершенные дипломные работы (1 экземпляр), удовлетворяющие необходимым требованиям;
- отзывы научных руководителей;

- рецензии на дипломные работы;
- сведения об успеваемости студентов (сводная ведомость);
- аттестационные листы, подтверждающие освоение обучающимися компетенций при изучении теоретического материала и прохождении практики по каждому из видов профессиональной деятельности;
- характеристики с оценкой из организации (предприятия) о прохождении преддипломной практики;
- отчеты о ранее достигнутых результатах, дополнительные сертификаты, свидетельства (дипломы) олимпиад, конкурсов, творческие работы по специальности;
- зачетные книжки студентов;
- книга протоколов заседаний ГЭК.

5.1.2. После завершения студентом работы и окончательного оформления текста дипломная работа представляется руководителю. Руководитель дает развернутый отзыв, в котором отмечает:

- актуальность темы;
- структура и полнота изложения рассматриваемых вопросов в теоретическом и практическом плане;
- теоретическая и практическая значимость результатов исследования;
- замечания по дипломной работе;
- отношение дипломника к выполнению дипломной работе общая оценка дипломной работы.

5.1.3. Студент-дипломник представляет работу на обязательное рецензирование. Образец рецензии представлен в методических рекомендациях к дипломным работам.

В качестве рецензентов могут выступать преподаватели или сотрудники смежных кафедр Института или других вузов, предприятий, организаций, имеющие высшее образование и работающие на руководящих должностях в сфере информационной безопасности.

5.1.4. В рецензии обязательно дается оценка выпускной работы по четырехбалльной системе (отлично, хорошо, удовлетворительно, неудовлетворительно).

5.1.5. В отзывах руководителей и рецензентов в заключении указывается, что автор (ФИО) выпускной квалификационной работы достоин (или не достоин) присвоения ему квалификации «Техник по защите информации».

5.1.6. Внесение изменений в дипломную работу после получения рецензии не допускается.

5.1.7. Заведующий кафедрой в установленные сроки определяет возможность допуска данной работы к защите и ставит свою подпись на титульном листе работы.

5.2. Темы выпускных квалификационных работ

10.02.1 Тематика дипломных работ разрабатывается преподавателями общепрофессиональных дисциплин, профессиональных модулей и

междисциплинарных курсов по специальности 10.02.01 «Организация и технология защиты информации» Института, в том числе, осуществляющих научное руководство дипломными работами, и рассматривается предметной (цикловой) комиссией общепрофессиональных дисциплин и профессиональных модулей специальности «Организация и технология защиты информации».

5.2.1. Тематика дипломной работы должна соответствовать содержанию одного или нескольких профессиональных модулей. Тема выпускной квалификационной работы может быть предложена студентом при условии обоснования им целесообразности ее разработки. При этом тематика дипломной работы должна соответствовать содержанию одного или нескольких профессиональных модулей, входящих в ППССЗ по специальности 10.02.01 «Организация и технология защиты информации».

5.2.2. Закрепление тем дипломных работ (с указанием научных руководителей и оппонентов) за студентами оформляется приказом ректора Института.

5.2.3. Научное руководство дипломной работой регламентируется Положением о итоговой аттестации по образовательным программам среднего профессионального образования выпускников Института.

5.2.4. Научный руководитель (далее - руководитель), а, при необходимости, научный консультант дипломной работы назначается приказом ректора Института.

5.2.5. Основными функциями руководителя дипломной работы являются:

- разработка индивидуальных заданий;
- консультирование по вопросам содержания и последовательности выполнения дипломной работы;
- оказание помощи студенту в подборе необходимой литературы и источников;
- контроль хода выполнения дипломной работы;
- подготовка письменного отзыва на дипломную работу.

5.2.6. Задания к дипломным работам определяют основное содержание, примерный объем, сроки сдачи дипломной работы, подписываются дипломником, руководителем дипломной работы и утверждаются заведующим кафедрой организации и технологии защиты информации.

5.2.7. По завершении студентом дипломной работы выпускник и научный руководитель подписывают ее и вместе с письменным отзывом и рецензией оппонента передают на кафедру.

5.2.8. Примерная тематика дипломных работ:

1. Организация безопасного удаленного доступа к ЛВС предприятия (название предприятия).
2. Построение защищенной виртуальной сети на базе специализированного программного обеспечения на предприятии (название

предприятия).

3. Автоматизация учета конфиденциальных документов на предприятии (название предприятия).

4. Организация процессов мониторинга конфиденциального документооборота на предприятии (название предприятия).

5. Разработка КСЗИ предприятия (название предприятия).

6. Организация системы планирования и контроля функционирования КСЗИ на предприятии (название предприятия).

7. Разработка структурно-функциональной модели управления КСЗИ предприятия (наименование предприятия).

8. Разработка системы программно-аппаратной защиты информации предприятия (наименование предприятия).

9. Разработка изолированной программно-аппаратной среды в Windows 8 (Windows 7, Linux и т.д.) (наименование предприятия).

10. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии (название предприятия).

11. Обоснование и разработка мер организационной защиты конфиденциальной информации при взаимодействии сотрудников предприятия

со сторонними организациями (название предприятия).

12. Разработка методов и форм работы с персоналом предприятия, допущенным к конфиденциальной информации (название предприятия).

13. Обоснование и разработка требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники и информационными системами (название предприятия).

14. Организация порядка установления внутриобъектного режима на объекте информатизации (название предприятия).

15. Организация защиты персональных данных (название предприятия).

16. Разработка и анализ эффективности внедрения мер по защите информации объектов, подключенных к глобальной сети (название предприятия).

17. Разработка организационно-технических мероприятий по обеспечению безопасности функционирующей информационно-вычислительной системы при вводе в эксплуатацию (внедрении) ее дополнительных очередей (подсистем) сторонними организациями (название предприятия).

18. Разработка рекомендаций по созданию комплексной системы защиты информации на предприятии (название предприятия).

19. Разработка комплексной системы защиты информации (название предприятия) с разработкой подсистемы видеонаблюдения.

20. Разработка комплексной системы защиты информации (название предприятия) с разработкой подсистемы охрано-пожарной системы.

21. Разработка комплексной системы защиты информации (название предприятия) с разработкой подсистемы защищенной связи.
22. Разработка комплексной системы защиты информации (название предприятия) с разработкой виброакустической защиты выделенного помещения.
23. Оценка защищенности помещения хозяйствующего субъекта (на конкретном примере) от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам.
24. Разработка комплекса рекомендаций по технической защите конфиденциальной информации хозяйствующего субъекта (на конкретном примере).
25. Разработка и обоснование требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники.
26. Разработка методов передачи и защиты информации в каналах связи.
27. Комплексная оценка защищенности помещения хозяйствующего субъекта (на конкретном примере) от утечки конфиденциальной информации по техническим каналам.
28. Разработка и обоснование требований и процедур по защите базы данных на предприятии.
29. Разработка системы защиты информации при межсетевом взаимодействии в организации (название организации).
30. Разработка виртуальной защищенной сети на базе ПО VipNet (или другого программного обеспечения) (название организации).
31. Методы применения антивирусных средств защиты информации.
32. Методы применения средств межсетевого экранирования.
33. Разработка комплекса мероприятий (рекомендаций) по защите информации, циркулирующей в защищаемых помещениях хозяйствующего субъекта (на конкретном примере).

Примечание.

По каждой теме обязательно указывать без скобок полное наименование предприятия (без сокращения), для которого проводится разработка.

6. Перечень литературы и иных источников для подготовки к итоговой аттестации

1. Алексеев, С.В. Правовое регулирование предпринимательской деятельности: учебное пособие / С.В. Алексеев. - М.: Юнити-Дана, 2015. - 502 с. Рекомендовано УМЦ.
<http://biblioclub.ru/index.php?page=book&id=114493>
1. Басаков М.И. Документационное обеспечение управления (делопроизводство): Учебник для студентов образовательных учреждений среднего профессионального образования. – Ростов н/Д.:

- Издательство «Феникс», 2013.-350 с.
2. Вычислительные системы, сети и телекоммуникации: учебное пособие. / А.П. Пятибратов, -М.: Издательство «КноРус», 2013.-376 с.: ил.
 3. Гребенюк Е.И., Гребенюк Н.А. Технические средства информатизации. Учебник. 8-е изд., стер. –М.: Издательский центр «Академия», 2013.-352 с. – (Серия: «Среднее профессиональное образование»).
 1. Ефремов, И. Информационные технологии в сфере безопасности: практикум: И. Ефремов, В. Солопова; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Оренбургский государственный университет». - Оренбург: ОГУ, 2013. - 116 с.
<http://biblioclub.ru/index.php?page=book&id=259178>
 1. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций / Ю.Н. Загинайлов. - М.: Берлин: Директ-Медиа, 2015. - 105 с.: ил. - Библиогр. в кн.
<http://biblioclub.ru/index.php?page=book&id=362895>
 4. Карпенков, С.Х. Технические средства информационных технологий: учебное пособие / С.Х. Карпенков. - 3-е изд., испр. и доп. - М.: Берлин: Директ-Медиа, 2015. - 376 с.: ил., табл. - Библиогр. в кн. Допущено МО РФ <http://biblioclub.ru/index.php?page=book&id=275367>
 5. Лапина, М.А. Информационное право: учебное пособие / М.А. Лапина, А.Г. Ревин, В.И. Лапин; под ред. И.Ш. Килясханов. - М.: Юнити-Дана, 2015. - 336 с. Рекомендовано УМЦ
<http://biblioclub.ru/index.php?page=book&id=118624>
 6. Некраха, А.В. Организация конфиденциального делопроизводства и защита информации: учебное пособие / А.В. Некраха, Г.А. Шевцова; Институт информационных наук и технологий безопасности, Российский государственный гуманитарный университет. - М.: Академический проект, 2012. - 222 с. Рекомендовано УМО.
<http://biblioclub.ru/index.php?page=book&id=143604>
 2. Нестеров, С.А. Основы информационной безопасности: учебное пособие / С.А. Нестеров; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб: Издательство Политехнического университета, 2014. - 322 с.: схем, табл., ил.
<http://biblioclub.ru/index.php?page=book&id=363040>
 7. Организация безопасной работы информационных систем: учебное пособие / Ю.Ю. Громов, Ю.Ф. Мартемьянов, Ю.К. Букурако и др.; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2014. - 132 с.: ил. Утверждено УС.

- <http://biblioclub.ru/index.php?page=book&id=277794>
8. Персианов, В.В. Электронное офисное делопроизводство: учебник / В.В. Персианов, Е.З. Киреева, М.Н. Казакова. - М.: Берлин: Директ-Медиа, 2016. - 326 с.: ил. Рекомендовано УМЦ
<http://biblioclub.ru/index.php?page=book&id=434743>
 9. Попович, Е. Документационное обеспечение управления персоналом: учебное пособие / Е. Попович; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Оренбургский государственный университет». - Оренбург: ОГУ, 2014. - 112 с. <http://biblioclub.ru/index.php?page=book&id=259328>
 10. Пятибратов, А.П. Вычислительные системы, сети и телекоммуникации: учебник / А.П. Пятибратов, Л.П. Гудыно, А.А. Кириченко. - 4-е изд., перераб. и доп. - М.: Финансы и статистика, 2013. - 736 с. Рекомендовано МО РФ
<http://biblioclub.ru/index.php?page=book&id=220195>
 11. Рогожин, М.Ю. Документационное обеспечение управления: учебно-практическое пособие / М.Ю. Рогожин. - М.: Берлин: Директ-Медиа, 2014. - 384 с. <http://biblioclub.ru/index.php?page=book&id=253704>
 2. Румынина В.В. Правовое обеспечение профессиональной деятельности: Учебник. 9-е изд. стер., - М.: Издательский центр «Академия», 2013.-224 с.
 12. Фомин, Д.В. Компьютерные сети: учебно-методическое пособие по выполнению расчетно-графической работы: учебно-методическое пособие / Д.В. Фомин. - М.: Берлин: Директ-Медиа, 2015. - 66 с.: ил. <http://biblioclub.ru/index.php?page=book&id=349050>
 2. Шаньгин П.П. Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М.: Издательство «Форум», 2013.-416 с. Рекомендовано МО РФ.